

Cybersecurity: Operational Resilience



Certification Training



Knowledge Sharing



Continuous Learning



Mission Assistance

Date: 24 February 2016

Presenter: Paul Shaw, CISSP, GICSP, Security+, IEEE PSEM

Email Address: paul.shaw@dau.mil



RESILIENCY



Cyber resiliency – the ability of systems to anticipate, continue to operate correctly in the face of, recover from, and evolve to better adapt to advanced cyber threats

Security focuses on achieving the security objectives of confidentiality, integrity, & availability



TAKEAWAY

- Understanding Threat & System Environment to develop your cybersecurity “Operational Resilience”
- Articulating “tradeoffs” to prioritize and grade deployment of cybersecurity capabilities
- Understanding how to “fit” into the operational environment for overall contribution to Mission Assurance





FRAMING THE PROBLEM

The Threat

A person wearing a futuristic, glowing helmet and a dark uniform is shown from the chest up, holding a glowing tablet. They are positioned in a dark, atmospheric environment with a blue sky and clouds. Several drones are flying in the sky around them, some with glowing lights. The overall scene suggests a high-tech, military or surveillance context.

JANUARY
2014

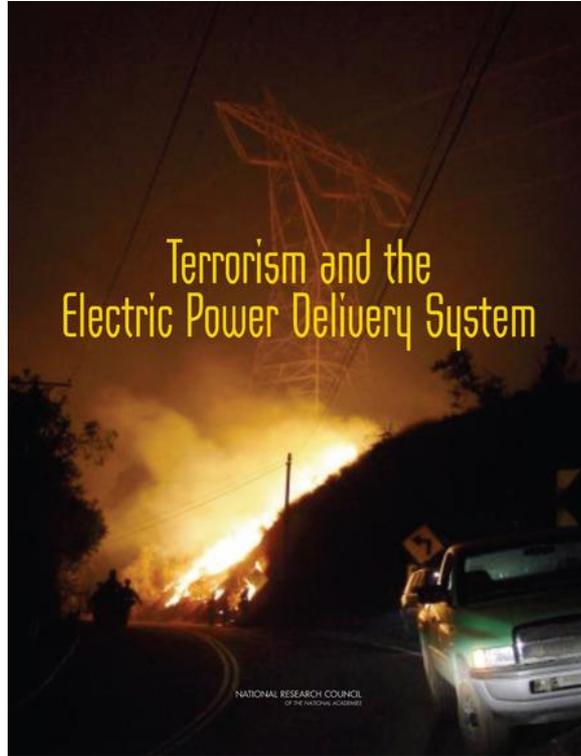
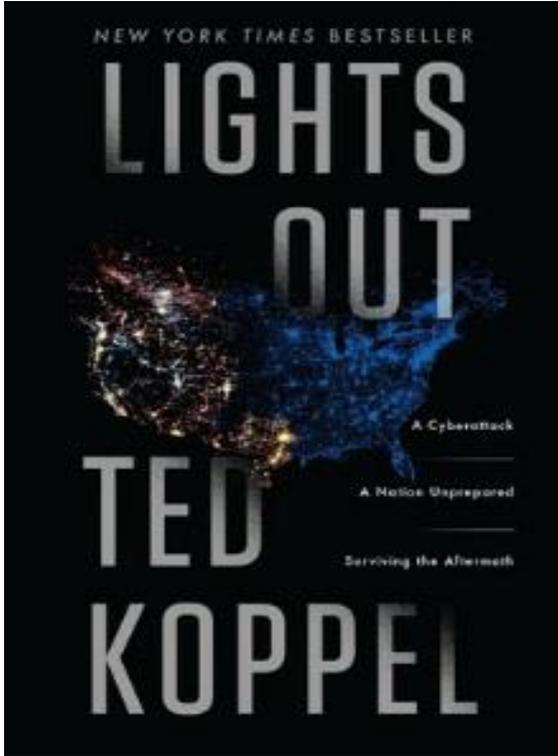
20YY
Preparing for War in the Robotic Age

By Robert O. Work and Shawn Brimley

The logo for the Center for a New American Security, featuring a shield with a red and white design and the text "Center for a New American Security" to its right.



IN THE NEWS



tce NEWS

Nuclear plants vulnerable to cyber attack

Report highlights issues including misconceptions about air-gapping

NUCLEAR power stations are facing an increasing threat from cyber attacks and aren't doing enough about it, according to a new report from current affairs think tank Chatham House.

The authors of the new report, *Cyber Security at Civil Nuclear Facilities: Understanding the Risks*, spoke to 30 industry practitioners, policy-makers and academics over 18 months to assess the security dangers and challenges facing the civil nuclear industry. Cyber attacks are of particular concern in the nuclear industry due to the radiation risk.

The report identifies several main problems at nuclear power stations. Strict regulatory requirements and concerns about the effects of new technology have meant that the industry was a late adopter

of digital systems and has less experience than other sectors. Executives are often unaware of the potential risks, and a focus on physical protection and safety has led to a lack of attention on cyber security.

The civil nuclear industry is increasingly using off-the-shelf software packages, which while cheaper, are more vulnerable to hacks. The researchers also found a pervasive myth that nuclear power stations are 'air-gapped'; in other words, not connected to the internet. However, many are, and even an air-gap can be easily breached with the use of a USB flash drive.

The report's authors say that there are a number of challenges, including insufficient spending on cyber security, communication difficulties between operators

and cyber security personnel, and a lack of cyber security training. They say it is difficult to study the extent of the problem as nuclear facilities often do not disclose incidents. There is also a lack of collaboration and learning from other industries.

The authors make general and specific recommendations. They say that the industry should formulate an organisational response that includes all levels of staff and all stakeholders, and an international management strategy for cyber security. It should implement the universal adoption of regulatory standards. The industry should encourage nuclear facilities to share threat information anonymously, without fear of penalisation, and promote conferences to develop relationships and share information. Regular



SABMiller and AB InBev will merge into world's largest brewer

SABMILLER has agreed to a \$67.5bn (US\$104.2b) takeover offer from AB InBev, clearing the way for the creation of a brewing giant responsible for the production of one in every three bottles of beer.

The £44 per share offer is a 50% premium on SABMiller's share price on 14 September, the day before speculation of a merger broke. SABMiller's board has recommended the offer – the fifth since AB InBev first offered £38 per share in September – and has asked the UK Takeover Panel to extend the formal deal deadline to 28 October. If AB InBev fails to formalise its offer, it will have to pay SABMiller a US\$3bn breakup fee.

If the deal goes ahead, the combined company would be responsible for more than 30% of the world's beer market, with its nearest largest rival Heineken trailing with 9.1%, according to data from Euromonitor.

The tie-up will bring together iconic brands including AB InBev's Budweiser and Stella Artois with SABMiller's Grolsch and Peroni. AB InBev employs more than 150,000 people in 24 countries while SABMiller employs 70,000 in more than 80 countries.

If successful, the merged company would be better placed to expand more quickly in key growth markets including Africa and South America, though would also have to sell off assets to gain approval from anti-monopoly authorities in their well-established markets such as China and the US.

Rumours that AB InBev would make a move for its smaller rival have circulated for years. SABMiller had a bid for Heineken rejected late last year, in what some suggested was a move to ward off an approach from AB InBev.

training should be in place at every facility, and personnel educated as to the risks of unauthorised devices and internet connections. Finally, cyber security should be built into all plans.

Keith Parker, the CEO of the Nuclear Industry Association, says that all security, including cyber security, is a priority of the nuclear industry. The UK's fleet is not presently digital and does not have embedded software open to hacking.

"Power station operators work closely with national agencies such as the Centre for the Protection of National Infrastructure and other intelligence agencies to always be aware of emerging threats," he adds. "Furthermore, the independent regulator continuously monitors and evaluates the safety of each plant alongside the operator to protect it from any outside threats and ensure the continued safe generation of low carbon electricity."

Critical Infrastructure needs to be Resilient



WE ARE VULNERABLE

Comments by ADM Rogers (Director NSA/US Cyber Command) to House (Select) Intelligence Committee on 20 November 2014

“There has been a lot of talk over the years about hypothetical dangers of a cyber Pearl Harbor, and it’s certainly become a bit of a cliché in cybersecurity circles. I would argue, however, that the threat of a catastrophic and damaging cyberattack in the United States critical infrastructure like our power or financial networks is actually becoming less hypothetical every day.

... Foreign cyberactors are probing Americans' critical infrastructure networks and in some cases have gained access to those control systems. Trojan horse malware that has been attributed to Russia has been detected on industrial control software for a wider range of American critical infrastructure systems throughout the country. This malware can be used to shut down vital infrastructure like oil and gas pipelines, power transmission grids and water distribution and filtration systems.

Not aware of a case yet where hackers gained access to one of these systems and used it to cause damage to American critical infrastructure, but I wouldn't take much comfort in that. I believe our advanced nation state adversaries have the ability to cause such damage. These nations lack a strong motive at this moment to conduct such an attack and are deterred only by the fear of U.S. retaliation. Our critical infrastructure networks are extremely vulnerable to such a damaging attack, and we can't count on a deterrence if we're already in an adversarial position with a nation like China or Russia. And we can't count on the fact that less rational actors might also gain access to those critical systems.” (Rogers, 2014, p. 3)



United States Government Accountability Office
Testimony
Before the Subcommittees on Energy and Research and Technology, Committee on Science, Space, and Technology, House of Representatives

For Release on Delivery
Expected at 10 a.m. ET
Wednesday, October 21, 2015

CRITICAL INFRASTRUCTURE PROTECTION

Cybersecurity of the Nation's Electricity Grid Requires Continued Attention

Statement of Gregory C. Wilshusen,
Director, Information Security Issues

GAO-16-174T

National Security Agency

Hearing of the House (Select) Intelligence Committee

Subject: "Cybersecurity Threats: The Way Forward"

Chaired By: Representative Mike Rogers (R-MI)

Witness:

Admiral Michael Rogers,
Commander, U.S. Cyber Command and
Director, National Security Agency

Location: 2212 Rayburn House Office Building, Washington, D.C.

Time: 9:00 am EST

Date: Thursday, November 20th, 2014

Transcript by
Federal News Service
Washington, D.C.



WHICH IS BIGGER

U. S. MARINE CORPS



End of FY 2015 - End Strength
of 182,100 Active Personnel*

End Strength from US Heritage.Org at
<http://index.heritage.org/military/2015/chapter/us-power/us-marine-corps/>

2015 - USMC is bigger by 2,100 than China's Cyber Warriors.
2018 - China's Cyber Warriors force could be bigger.



“State-sponsored cyber espionage is ubiquitous, with more than 100 countries actively hacking the systems of other countries and businesses. China alone has developed an army of 180,000 cyber spies and warriors.” (Goodman, 2015, p. 31)

Reference: Goodman, M. (2015). *Future Crimes: Everything Is Connected, Everyone Is Vulnerable, and What We Can Do About It*. Doubleday ISBN: 978-0-53900-5.



YOUR THREAT

Largest APT1 data theft
from a single organization:

6.5 Terabytes

over 10 months



APT1

Exposing One of China's Cyber
Espionage Units

TABLE 2: Two profession codes and university recommended courses for students intending to apply for positions in Unit 61398

Profession Code	Required Proficiencies
080902 — Circuits and Systems	<ul style="list-style-type: none"> » 101 — Political » 201 — English » 301 — Mathematics » 842 — Signal and Digital Circuits (or) 840 - Circuits » Interview plus a small written test: <ul style="list-style-type: none"> – Circuits and Systems-based professional knowledge and comprehensive capacity – Team spirit and ability to work with others to coordinate – English proficiency
081000 — Information and Communications Engineering	<ul style="list-style-type: none"> » 101 - Political » 201 - British [English] » 301 - Mathematics » 844 - Signal Circuit Basis

(p. 11)

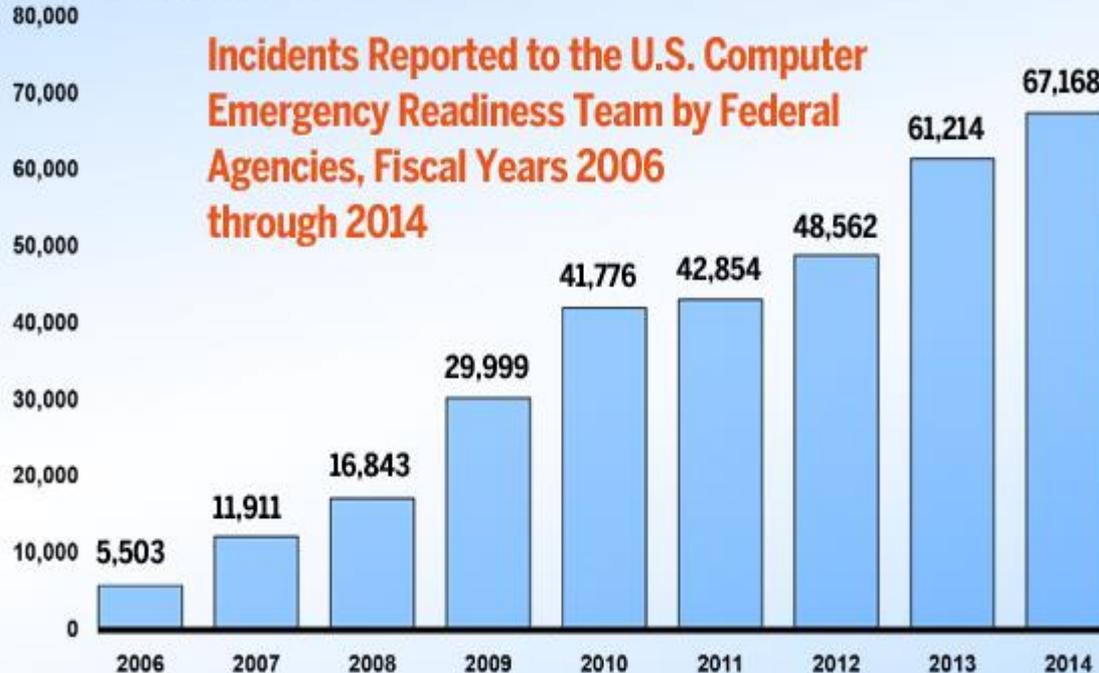
APT1 has systematically stolen hundreds of terabytes of data from at least 141 organizations, and has demonstrated the capability and intent to steal from dozens of organizations simultaneously.⁴



ATTACKS ARE INCREASING

Security incidents reported to U.S. Computer Emergency Readiness Team (US-CERT) - Increased 1,121 percent

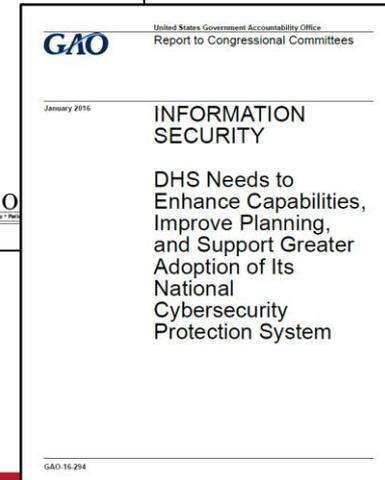
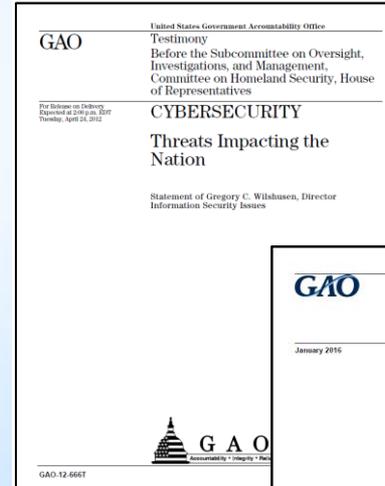
Number of reported incidents



Incidents Reported to the U.S. Computer Emergency Readiness Team by Federal Agencies, Fiscal Years 2006 through 2014

Fiscal year

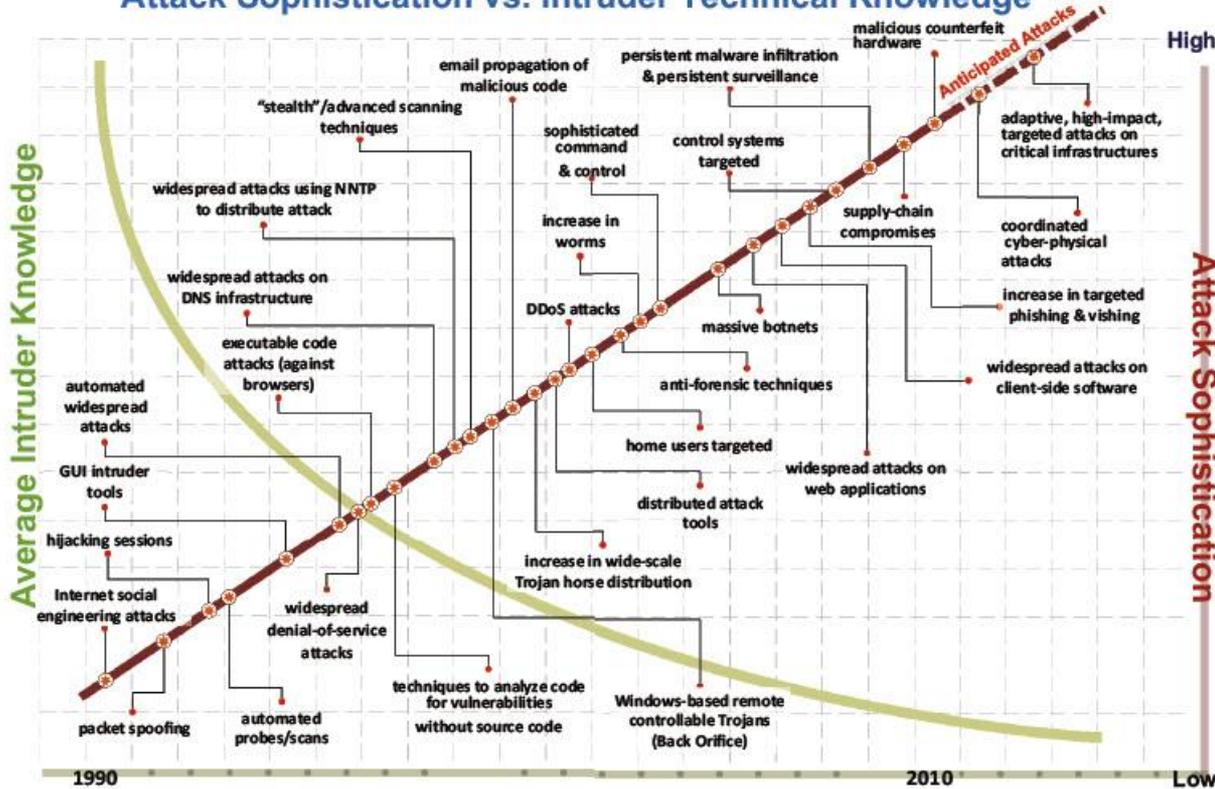
Source: GAO analysis of United States Computer Emergency Readiness Team data for fiscal years 2006-2014. | GAO-15-758T





LESS CAPABLE ATTACKERS - CAN DO MORE

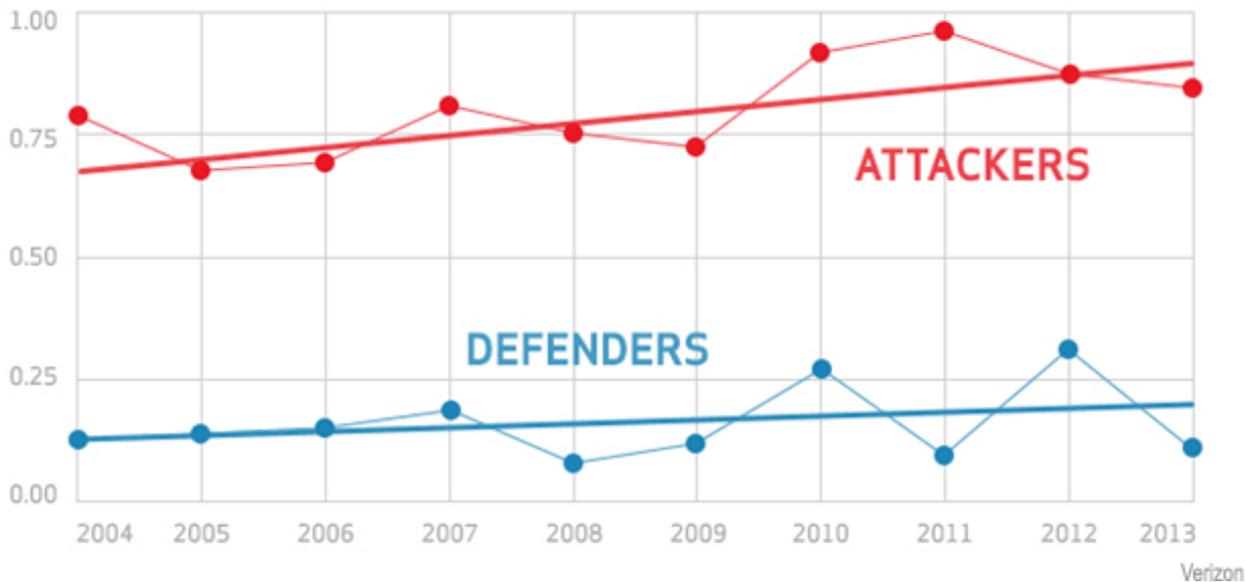
Attack Sophistication vs. Intruder Technical Knowledge



**Bottom Line:
Less Knowledgeable
Attackers can
execute Increasing
Sophisticated Attacks**



ATTACKERS HAVE THE ADVANTAGE



Verizon's 2014 Data Breach Investigations Report
Available at <http://www.verizonenterprise.com/DBIR>

Time from Earliest Evidence of Compromise to Discovery of Compromise

205

median number of days that threat groups were present on a victim's network before detection

↓ 24 days less than 2013

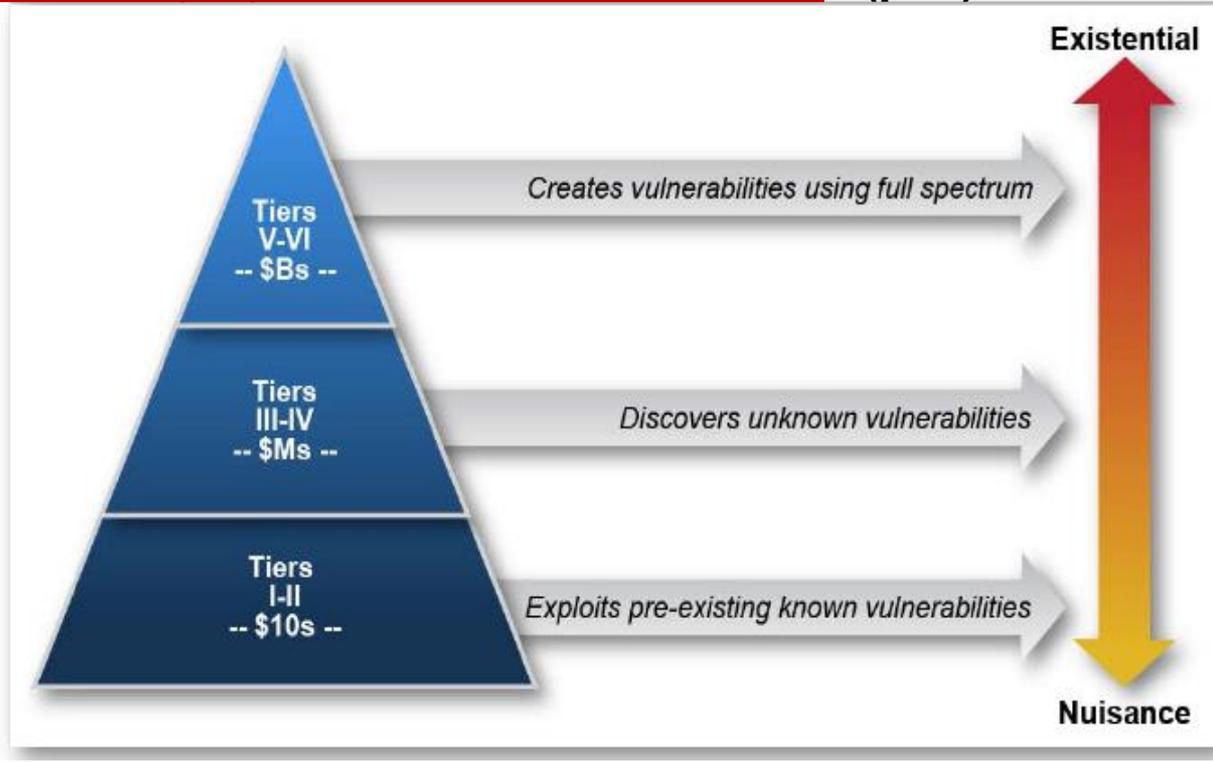
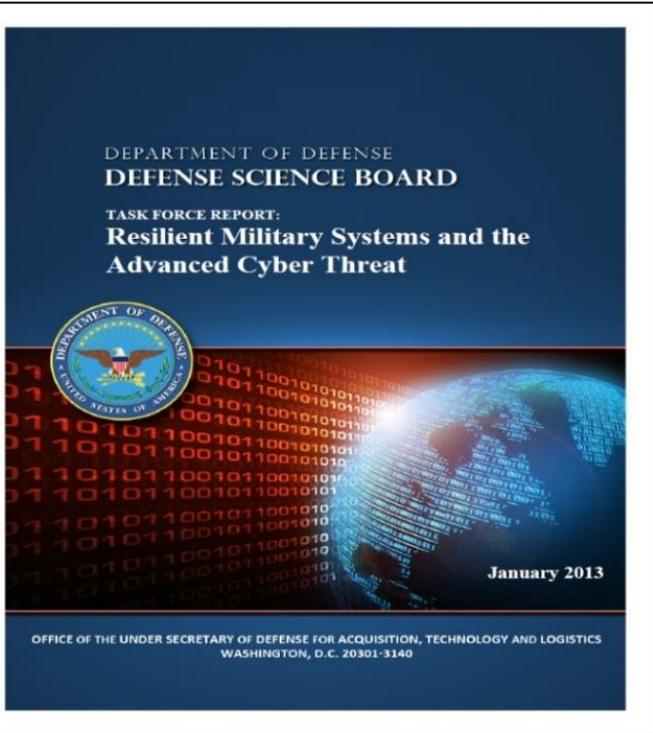
Longest Presence: 2,982 days

Days to Detect from Mandiant
2015 Report available at
<https://www2.fireeye.com/rs/fireeye/images/rpt-m-trends-2015.pdf>

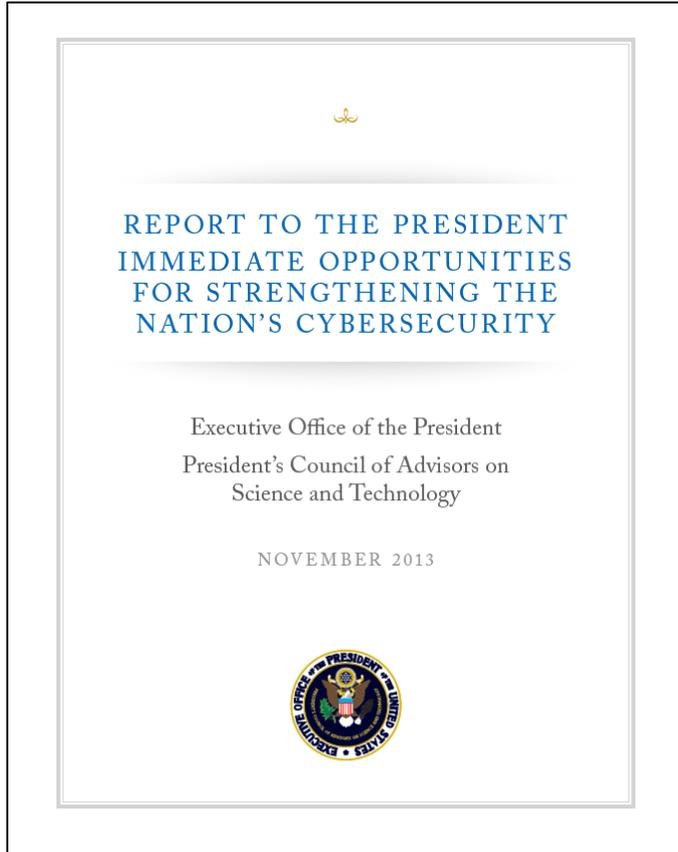


EXPECT CYBER ATTACKS

“The DoD should expect cyber attacks to be part of all conflicts in the future, and should not expect competitors to play by our version of the rules” (p. 5)



“Defense-only is a failed strategy.” (p. 6)



“Future architectures will need to start with the premise that each part of a system must be designed to operate in a hostile environment.” (p. 3)

“Cybersecurity ... requires a set of processes that must continuously couple information about an evolving threat to defensive reactions and responses.” (p. 6)



DEFINING RESILIENCE

What is Resilience?



TREND MICRO Organization of American States

Report on Cybersecurity and Critical Infrastructure in the Americas

Three Pillars for System Survivability KPP

Prevent

- **Reduced likelihood of being hit**
- Cyber equivalent: Prevent adversary from initiating cyber attack

Mitigate

- **Reduced vulnerability if hit**
- Cyber equivalent: Prevent cyber attack success

Resiliency

- **Complete the mission despite the loss**
- Cyber equivalent: Fight through cyber effects, limiting mission harm

RESILIENCY



Cyber resiliency – the ability of systems to anticipate, continue to operate correctly in the face of, recover from, and evolve to better adapt to advanced cyber threats

Security focuses on achieving the security objectives of confidentiality, integrity, & availability



OPERATIONAL RESILIENCE



Department of Defense INSTRUCTION

NUMBER 8500.01
March 14, 2014

DoD CIO

SUBJECT: Cybersecurity

References: See Enclosure 1

1. **PURPOSE.** This instruction:

- a. Reissues and renames DoD Directive (DoDD) 8500.01E (Reference (a)) as a DoD Instruction (DoDI) pursuant to the authority in DoDD 5144.02 (Reference (b)) to establish a DoD cybersecurity program to protect and defend DoD information and information technology (IT).
- b. Incorporates and cancels DoDI 8500.02 (Reference (c)), DoDD C-5200.19 (Reference (d)), DoDI 8552.01 (Reference (e)), Assistant Secretary of Defense for Networks and Information Integration (ASD(NII))/DoD Chief Information Officer (DoD CIO) Memorandums (References (f) through (k)), and Directive-type Memorandum (DTM) 08-060 (Reference (l)).
- c. Establishes the positions of DoD principal authorizing official (PAO) (formerly known as principal accrediting authority) and the DoD Senior Information Security Officer (SISO) (formerly known as the Senior Information Assurance Officer) and continues the DoD Information Security Risk Management Committee (DoD ISRMC) (formerly known as the Defense Information Systems Network (DISN)/Global Information Grid (GIG) Flag Panel).
- d. Adopts the term "cybersecurity" as it is defined in National Security Presidential Directive-54/Homeland Security Presidential Directive-23 (Reference (m)) to be used throughout DoD instead of the term "information assurance (IA)."

DoDI 8500.01 "Operational Resilience"

"Whenever possible, technology components (e.g., hardware and software) have the ability to reconfigure, optimize, self-defend, and recover with little or no human intervention." (p. 3)

"OPERATIONAL RESILIENCE. Operational resilience requires three conditions to be met: information resources are trustworthy; missions are ready for information resources degradation or loss; and network operations have the means to prevail in the face of adverse events." (p. 31)

Trustworthy, Ready for Degradation, Prevail



CYBERSPACE PERFORMANCE



Department of Defense INSTRUCTION

NUMBER 5200.44
November 5, 2012

DoD CIO/USD(AT&L)

SUBJECT: Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)

References: See Enclosure 1

1. **PURPOSE.** This Instruction, in accordance with the authorities in DoD Directive (DoDD) 5134.01 (Reference (a)) and DoDD 5144.1 (Reference (b)):

a. Establishes policy and assigns responsibilities to minimize the risk that DoD's warfighting mission capability will be impaired due to vulnerabilities in system design or sabotage or subversion of a system's mission critical functions or critical components, as defined in this Instruction, by foreign intelligence, terrorists, or other hostile elements.

b. Implements the DoD's TSN strategy, described in the Report on Trusted Defense Systems (Reference (c)) as the Strategy for Systems Assurance and Trustworthiness, through Program Protection and information assurance (IA) implementation to provide uncompromised weapons and information systems. The TSN strategy integrates robust systems engineering, supply chain risk management (SCRM), security, counterintelligence, intelligence, information assurance, hardware and software assurance, and information systems security engineering disciplines to manage risks to system integrity and trust.

A system's defensive cyberspace performance in the operational environment:

- Withstand representative cyber-attacks
- Detect and react to those attacks &
- Return to normal operations in the event of a successful cyber-attack

(DoD Instruction 5200.44)

Return to Normal Operations!!



NAVY'S CYBER RESILIENCY



UNCLASSIFIED

Warfighting First – Operate Forward – Be Ready



Cyber Resiliency Approach

NSA's Top 10 IA Mitigation Strategies

Mitigation Strategies	Mitigation Goal Areas			
	Device Integrity	Damage Containment	Defense of Accounts	Secure & Available Transport
Application Whitelisting	■			
Control Administrative Privileges		■	■	■
Limit Workstation-to-Workstation Communication		■		■
Use Anti-Virus File Reputation Services	■			
Enable Anti-Exploitation Features	■			
Implement Host Intrusion Prevention System (HIPS) rules	■			
Set a Secure Baseline Configuration	■			
Use Web Domain Name System (DNS) Reputation	■			■
Take Advantage of Software Improvements	■			
Segregate Networks and Functions		■		■

Industry Recommendations (Controls against Cyber Espionage)

RECOMMENDED CONTROLS

Having received news of an espionage-related breach is a lot of anger, but DAU's cyber resilience working group and attendees here are ready to discuss the next steps. The next step is to determine what the group learned, what the cause was, and what the group can do to prevent a similar incident from happening again. This is not a simple task, but it is a critical one. The group will be looking for ways to improve its cyber resilience and to prevent a similar incident from happening again.

Break the delivery-exploitation-installation chain

Identify the chain of events that led to the breach and break it at as many points as possible. This might include identifying the source of the exploit, the way the exploit was delivered, and the way the exploit was installed. This is a complex task, but it is a critical one. The group will be looking for ways to improve its cyber resilience and to prevent a similar incident from happening again.

Patch ALL THE THINGS!

Plan and budget for patches to protect our systems. A common belief is that patches are a waste of money. However, patches are a critical part of our cyber resilience. We must ensure that we have a process in place to identify, test, and deploy patches in a timely and secure manner.

Use and update anti-virus (AV)

Use anti-virus software to detect and prevent malware. Update the signatures regularly to ensure that the software is able to detect and prevent the latest threats.

Spot C2 and data exfiltration

Use network monitoring tools to detect and prevent command and control (C2) and data exfiltration. This is a complex task, but it is a critical one. The group will be looking for ways to improve its cyber resilience and to prevent a similar incident from happening again.

Train users

Train users on how to recognize and report suspicious activity. This is a critical part of our cyber resilience. We must ensure that our users are aware of the risks and know how to protect themselves.

Segment your network

Segment your network to limit the impact of a breach. This is a critical part of our cyber resilience. We must ensure that we have a process in place to identify, test, and deploy network segmentation in a timely and secure manner.

Stop lateral movement inside the network

Use network monitoring tools to detect and prevent lateral movement. This is a critical part of our cyber resilience. We must ensure that we have a process in place to identify, test, and deploy network monitoring in a timely and secure manner.

Keep good logs

Keep good logs to help with incident response. This is a critical part of our cyber resilience. We must ensure that we have a process in place to identify, test, and deploy logging in a timely and secure manner.

Cyber Resiliency Approach

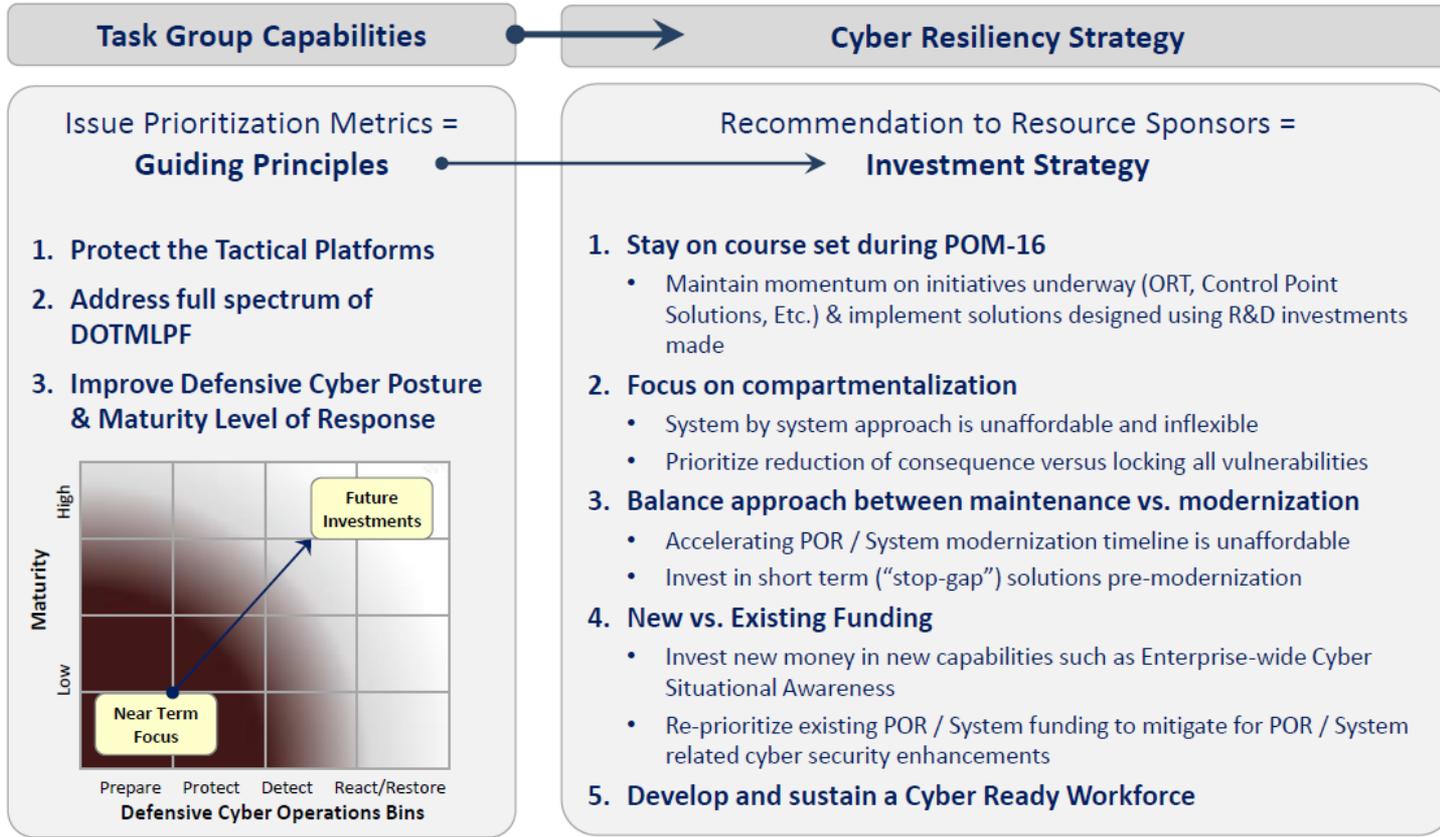
- Control Points:** Control Points will allow us to effectively isolate portions of our networks and prevent adversaries who gain a foothold from moving laterally. Also improve boundary defenses for individual portions of the network and serve as insertion points in the network for emerging technology solutions.
- Cyber Situational Awareness (SA):** Allow us to visualize the activity in the "cyber-field", promote timely assessment of normal vs. abnormal activity, and mitigate possible threats. Cyber SA provides us with the tools to detect and respond to higher level threat actors.
- Designing (vice retroactively Patching-in) Resiliency within Systems & Networks:** Generating common sets of standards and protocols to improve our cyber posture by driving down variance, and also designing-in resiliency in future system designs.
- Cyber Hygiene:** Use of focused Tactics, Techniques & Procedures (TTPs) and workforce training
- Cyber Ready Workforce:** Improving manning levels, personnel training and Fleet readiness via readiness reviews, Fleet cyber security efforts, Cybersecurity Workforce continuing education, unit patch/scan compliance and adherence to computer tasking orders (CTO).

- Control Points
- Cyber Situational Awareness
- Designing Resiliency
- Cyber Hygiene
- Cyber Ready Workforce

Leveraged Stakeholder, Community and Industry recommendations to develop Enterprise Approach



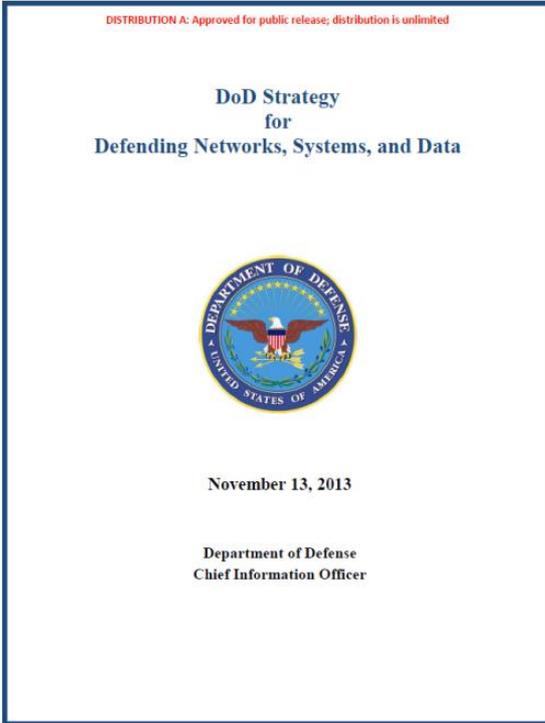
NAVY'S CYBER RESILIENCE



Deliver a realistic and executable requirement to the Resource Sponsors that improves our Enterprise wide Cyber Resiliency both effectively and efficiently



DOD CYBER GOALS



Focus Areas	Critical Elements
Establish a Resilient Cyber Defense Posture	<ul style="list-style-type: none">• Architect a Defensible Information Environment• Enhance Security through Cyber Hygiene and Best Practices• Strengthen Data Defenses• Increase Focus on Industrial Control Systems and Embedded Computing• Institutionalize Threat-Based Engineering and Acquisition
Transform Cyber Defense Operations	<ul style="list-style-type: none">• Improve Active Cyber Defense Capabilities• Mitigate All Phases of Cyber Aggression• Ready Forces to Maneuver• Employ Unpredictable Defenses
Enhance Cyber Situational Awareness	<ul style="list-style-type: none">• Improve the Cyber Sensing Infrastructure• Harness the Power of Big Data Analytics• Implement a Multi-Mission Cyber Operational Picture• Increase Information Sharing and Cooperation
Assure Survivability against Highly-Sophisticated Cyber Attacks	<ul style="list-style-type: none">• Assure Survivability of High Priority Mission Areas• Prepare for Success Against Large-Scale Cyber Attacks• Quickly Regenerate Cyber Capabilities

“Establish a Resilient Cyber Defense Posture

The first strategic imperative, establishing a resilient cyber defense posture, will be achieved through personal security practices, architecture and engineering, and delivery of new capabilities and solutions to address shortfalls in the current DoD Information and Communication Technology (ICT) infrastructure rapidly.” (p. 2)



NIST CYBERSECURITY FRAMEWORK

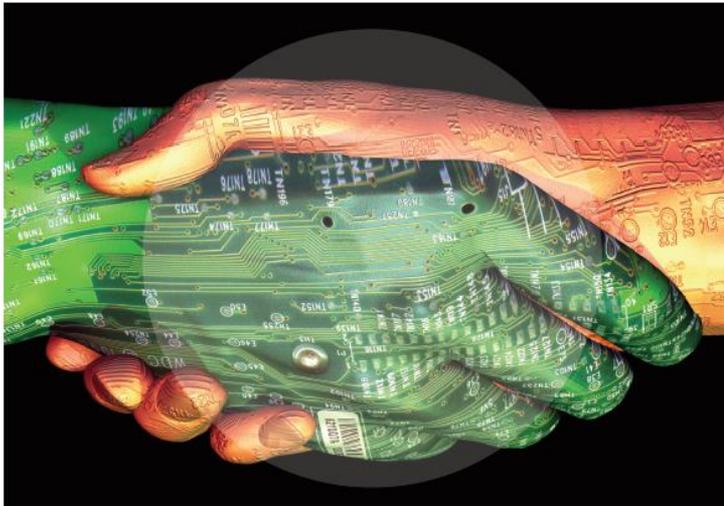
Respond – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

Recover – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

Partnering for Cyber Resilience

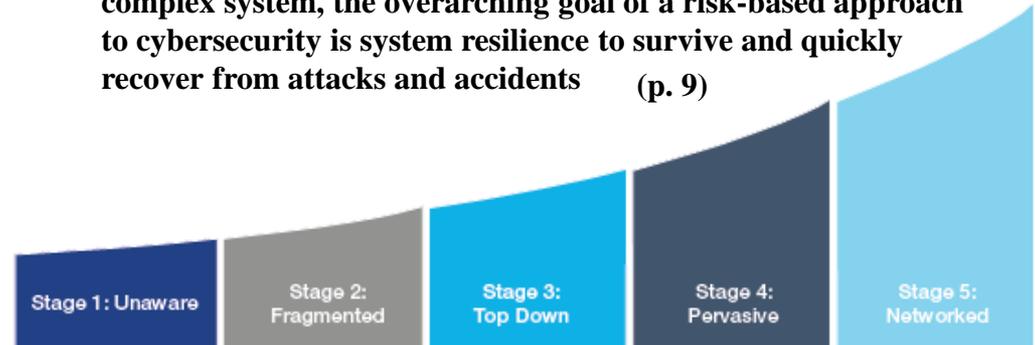
Risk and Responsibility in a Hyperconnected World - Principles and Guidelines



Principles for Cyber Resilience

Starting Assumptions:

- The interdependence of all organizations within the online environment provides a foundational assumption for all cyber risk management
- Improving cyber risk management practices within a single organization contributes to global cyber resilience
- A risk-based approach is an efficient and effective approach to deal with cyber threats
- Recognizing that 100% risk mitigation is not possible in any complex system, the overarching goal of a risk-based approach to cybersecurity is system resilience to survive and quickly recover from attacks and accidents (p. 9)



Maturity Model for Cyber Resilience



SECURITY & RESILIENCE

Security with Resilience





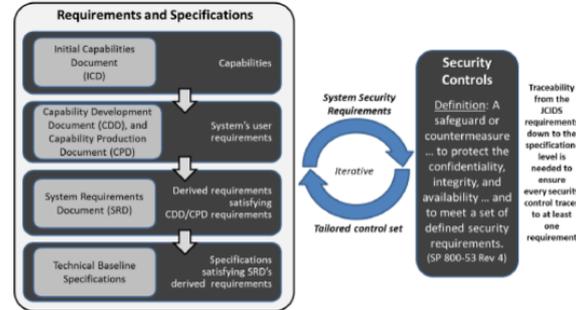
SECURITY CONTROLS

When monitoring risks:

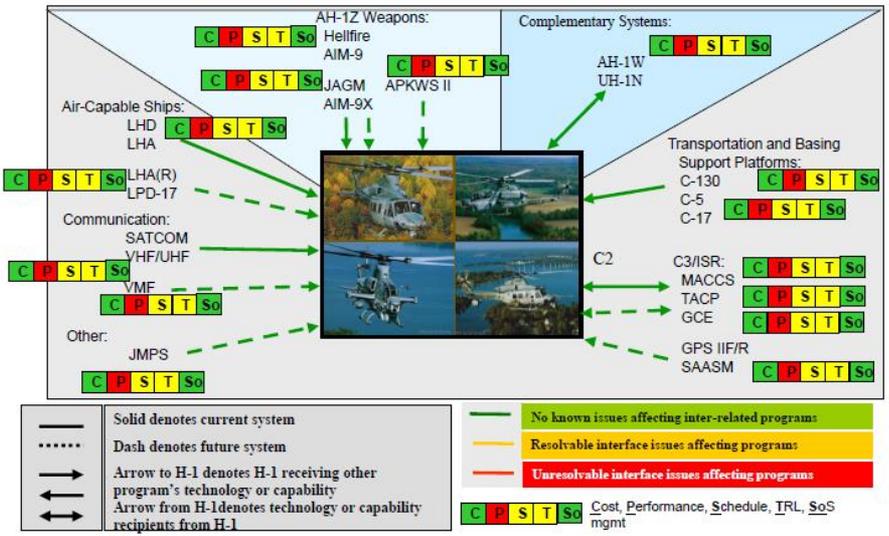
- Include Technical Performance Measures (TPMs) as an integral activity when monitoring risks after selecting the appropriate risk handling strategy
- Conduct regular status updates to monitor risks for changes to likelihood or consequences
- Document risks that can be retired as well as risks that are still being managed to avoid unnoticed relapse of the retired risk
- Keep lines of communication open to notify management when ability to handle the risk is out your control



Relationship Between Requirements, Specifications and Security Controls



Controls are a form of protection; they do not provide for every possible type of protection. Requirements and Specifications reflect design trades and implementation details of Security Controls.



Department of Defense
Risk, Issue, and Opportunity Management Guide
for Defense Acquisition Programs

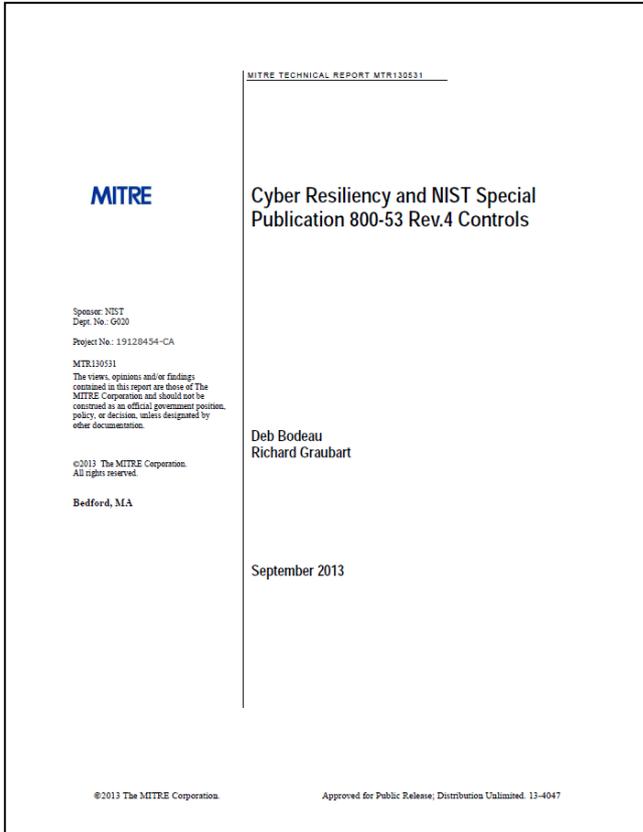
June 2015

Office of the Deputy Assistant Secretary of Defense for
Systems Engineering

Washington, D.C.



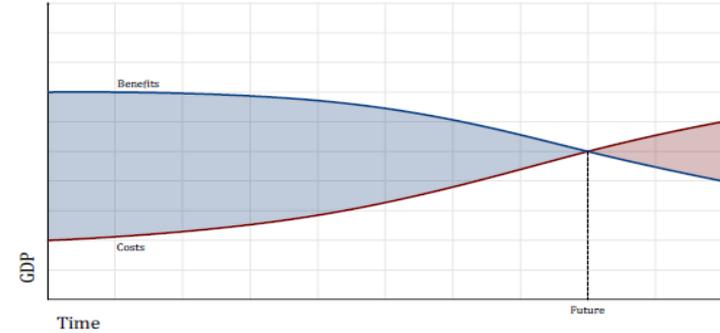
SECURITY OR RESILIENCE



NIST SP 800-53R4 has over 860 control and enhancements. Not surprisingly, the majority of controls in NIST 800-53R4 are not resiliency oriented. Rather the bulk of the controls are oriented to achieving the information system security goals of confidentiality, integrity, and availability. Still, approximately 17% of the controls⁷ in NIST 800-53R4 are cyber resiliency oriented. But because of the sheer number of controls it is not easy to identify which controls support resiliency and for those that do support resiliency, what aspect of resiliency do they support. Such identification is needed for those developing system requirements as well as resiliency overlays. Appendix A provides this identification.

Do you understand your tradeoffs Between security and resilience?

Cyber Resiliency and NIST Special Publication 800-53 Rev.4 Controls available at
<http://www.mitre.org/sites/default/files/publications/13-4047.pdf>



THE FREDERICK S. PARDEE CENTER FOR INTERNATIONAL FUTURES
EXPLORE, UNDERSTAND, SHAPE

Cyber Benefits and Risks:
 Quantitatively Understanding and Forecasting the Balance

Extended Project Report from the
 Frederick S. Pardee Center for International Futures
 Josef Korbel School of International Studies
 University of Denver
www.pardee.du.edu
 September 2015

Barry B. Hughes, David Bohl, Mohammad Irfan, Eli Margolese-Malin, and José Solórzano

In project collaboration with

ZURICH
 INSURANCE

and the

Atlantic Council

Risk Nexus
 Overcome by cyber risks? Economic benefits and costs of alternate cyber futures

FEDERAL CYBERSECURITY RESEARCH AND DEVELOPMENT STRATEGIC PLAN
 ENSURING PROSPERITY AND NATIONAL SECURITY

National Science and Technology Council
 Networking and Information Technology Research and Development Program

February 2016

“Current spending by firms in the U.S. may only prevent about 69 percent of potential attacks, however; warding off 95 percent might cost 8 times as much in defensive spending.” (Padee Center, p. 6)

“The current trajectories for benefit and risk are unsustainable. One recent report suggests the benefits may be overtaken by cybersecurity costs as early as 2030.” (Executive Office of the President, p. 4)



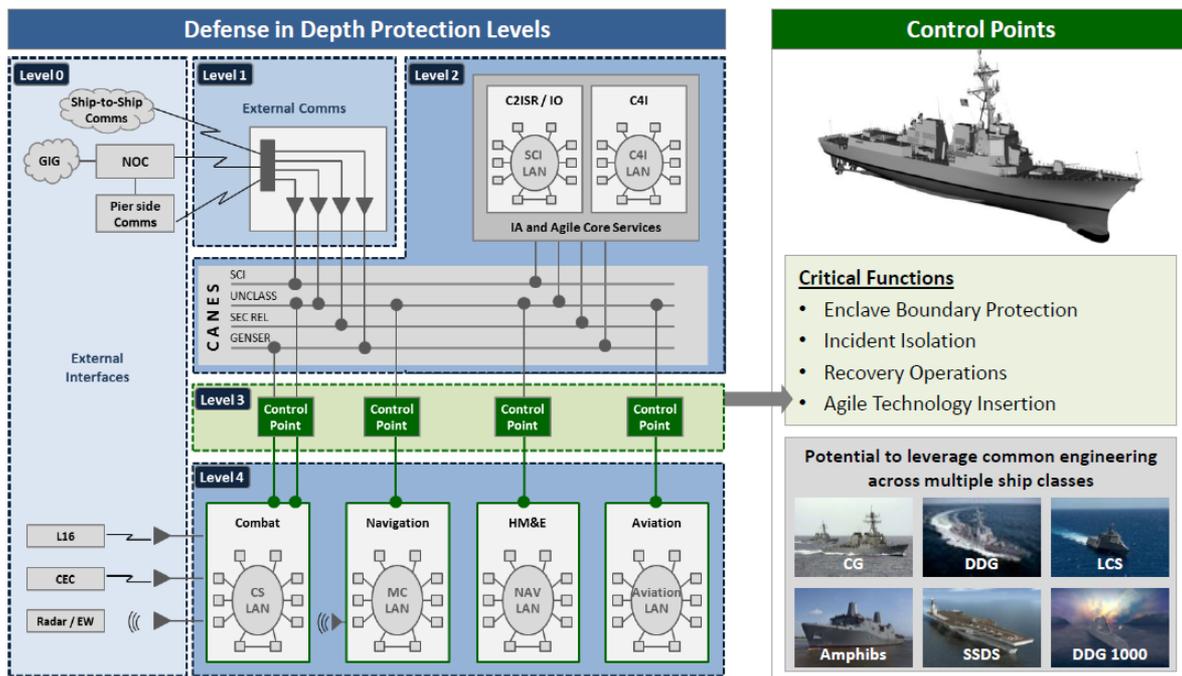
CONTROL POINTS

UNCLASSIFIED

Warfighting First – Operate Forward – Be Ready



Control Point Approach



- Containment of Compromise
- Isolation between Enclaves
- Recovery Strategy

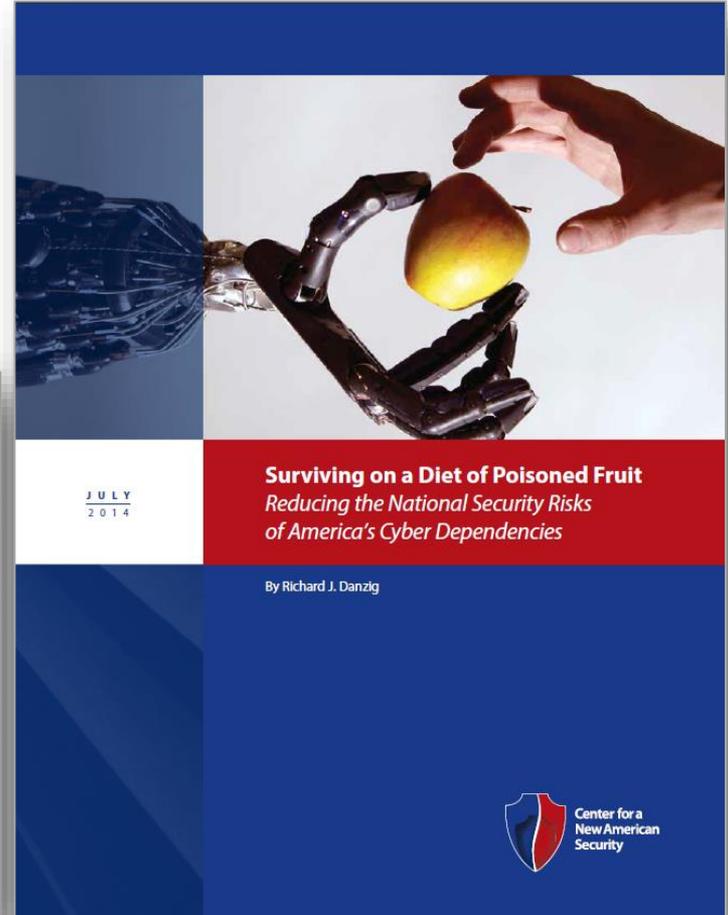
Control Points will allow us to effectively segment portions of our shipboard network, add greater ability to maneuver through intrusions, and ensure mission assurance

Assured C2 – Battlespace Awareness – Integrated Fires



RESILIENCE

Resilience Framework





MITRE'S RESILIENCE FRAMEWORK

MITR140409R1

MITRE

Cyber Resiliency Engineering Aid –
The Updated Cyber Resiliency
Engineering Framework and
Guidance on Applying Cyber
Resiliency Techniques

The views, opinions and/or findings contained in this report are those of The MITRE Corporation and should not be construed as an official government position, policy, or decision, unless designated by other documentation.
Approved for Public Release
Distribution Unlimited
PR 15-1334

©2015 The MITRE Corporation.
All rights reserved.

Deborah Bodeau
Richard Graubart
William Heinbockel
Ellen Laderman
May 2015

Bedford, MA

Goal	Description
Anticipate	Maintain a state of informed preparedness for adversity
Withstand	Continue essential mission/business functions despite adversity
Recover	Restore mission/business functions during and after adversity
Evolve	Adapt mission/business functions and/or supporting capabilities to predicted changes in the technical, operational, or threat environments

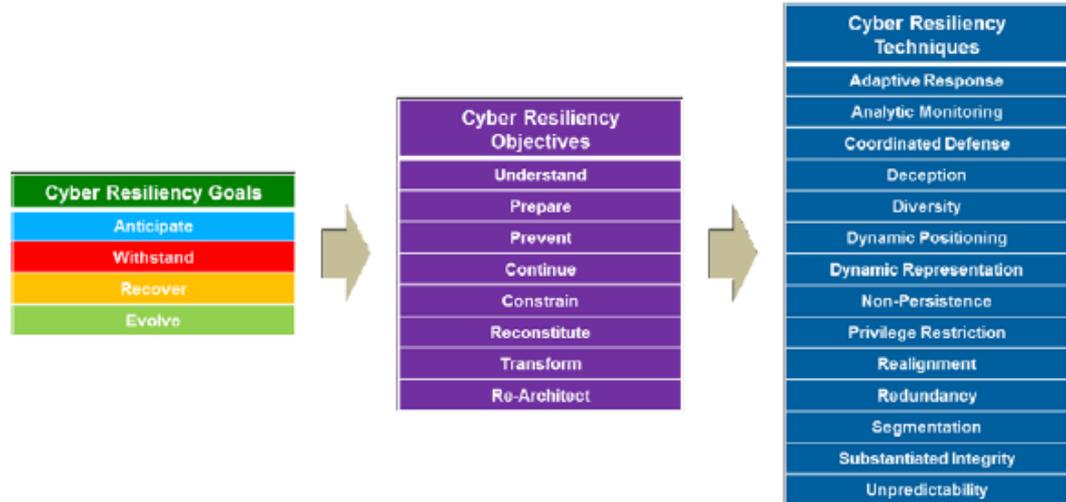


Figure 2. Cyber Resiliency Engineering Framework



RESILIENCE TECHNIQUES

Common Resiliency techniques are listed by phase (below) and representative approaches (right)

	Understand	Prepare	Prevent	Constrain	Continue	Reconstitute	Transform	Re-Architect
Adaptive Response				X	X	X		
Analytic Monitoring	X	X		X		X		
Coordinated Defense		X	X	X	X	X		
Deception	X		X		X			
Diversity			X		X			X
Dynamic Positioning	X		X		X			X
Dynamic Representation	X	X					X	
Non-Persistence			X	X	X			X
Privilege Restriction			X	X				
Realignment				X			X	
Redundancy					X	X		
Segmentation / Isolation			X	X				
Substantiated Integrity	X		X	X	X	X		
Unpredictability	X		X		X			

Cyber Resiliency Technique	Representative Approaches	
AR: Adaptive Response	Dynamic Reconfiguration Dynamic Resource Allocation Adaptive Management	
AM: Analytic Monitoring	Monitoring & Damage Assessment Sensor Fusion & Analysis Malware & Forensic Analysis	
CD: Coordinated Defense	Technical Defense-in-Depth Coordination & Consistency Analysis	
DC: Deception	Obfuscation Dissimulation / Disinformation Misdirection / Simulation	
DV: Diversity	Architectural Diversity / Heterogeneity Design Diversity / Heterogeneity Synthetic Diversity	Information Diversity Command, Control, and Communications Path Diversity Supply Chain Diversity
DP: Dynamic Positioning	Functional Relocation of Sensors Functional Relocation of Cyber Assets	Asset Mobility Distributed Functionality
DR: Dynamic Representation	Dynamic Mapping & Profiling Dynamic Threat Modeling Mission Dependency & Status Visualization	
NP: Non-Persistence	Non-Persistent Information Non-Persistent Services Non-Persistent Connectivity	
PR: Privilege Restriction	Privilege Management Privilege-Based Usage Restriction Dynamic Privileges	
RA: Realignment	Purposing Offloading / Outsourcing	Restriction Replacement
RD: Redundancy	Protected Backup & Restore Surplus Capacity Replication	
SG: Segmentation / Isolation	Predefined Segmentation Dynamic Segmentation / Isolation	
SI: Substantiated Integrity	Integrity / Quality Checks Provenance Tracking Behavior Validation	
UN: Unpredictability	Temporal Unpredictability Contextual Unpredictability	

1

2

3

4

5 **DRAFT**

6 **Framework for Cyber-Physical Systems**

7 **Release 0.8**

8

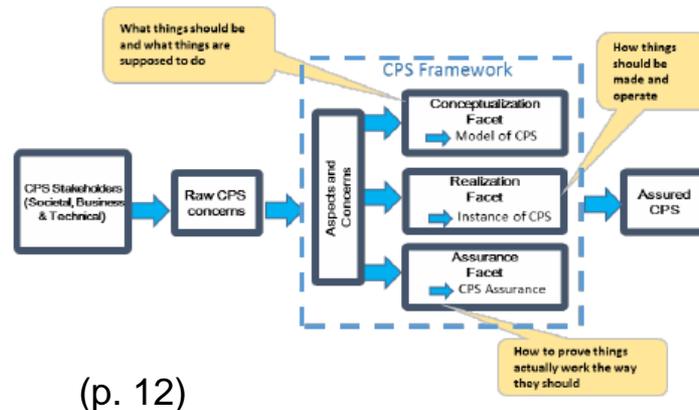
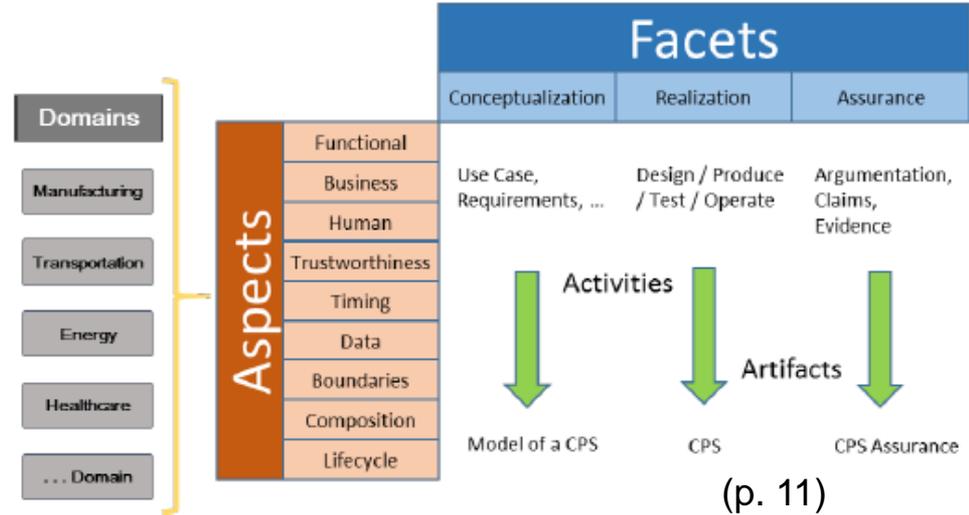
9 September 2015

10

11

12 Cyber Physical Systems Public Working Group

13





DSB RECOMMENDATIONS

Networks Inherently Self-defensible to Cyber Attack

At present, there are no known ways to fully protect cyber systems from malicious intrusion and potential damage or theft. Within the next decade, a number of well-attended and funded technologies and protocols are emerging and may be developed to significantly mitigate this problem. However, a near-term solution was identified in this study that may be useful for some focused and narrowly defined systems. A near-term demonstration project is proposed for a system architecture comprised of digital processors, data storage, and networks that is inherently self-defensible from cyber attack.

The proposed approach capitalizes on the fact that there are some critical infrastructure systems that have a unique set of characteristics that make them easier to defend. These systems include control systems for power grids, municipal water supplies, and air traffic control, and for some defense communication and mission command systems. While trust and availability of these systems are critical to national security, they tend to be less complex with moderate data transmission rates and the ability to withstand built-in microsecond delays to inputs and outputs.

The proposed solution uses a hardware chip to monitor the operation of the software operating system, regularly ensuring operating system software has not been modified. Because malicious modification of operating system software is the primary attack vector for cyber intrusions, compromising a system protected this way would become much more difficult and expensive. Creating trustworthy systems and periodically refresh it will force attackers to confront a moving target. The proposed approaches would make it more difficult and resource intensive for both external and insider attackers to successfully attack cyber systems.

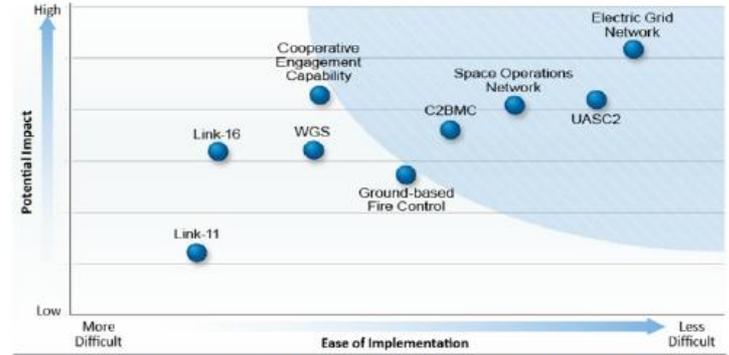


Figure 5 Potential Impact and Ease of Security Enhancement for Some Critical Systems Important to Defense Operations.

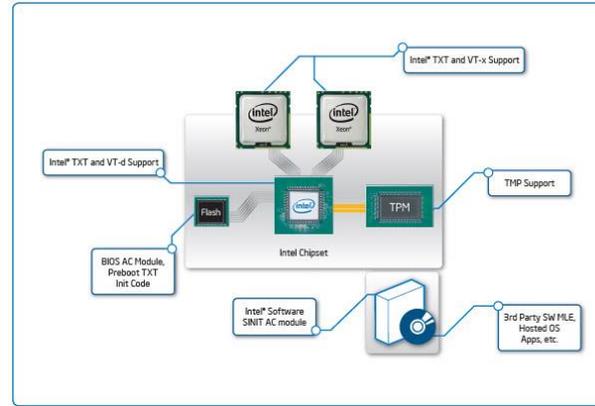
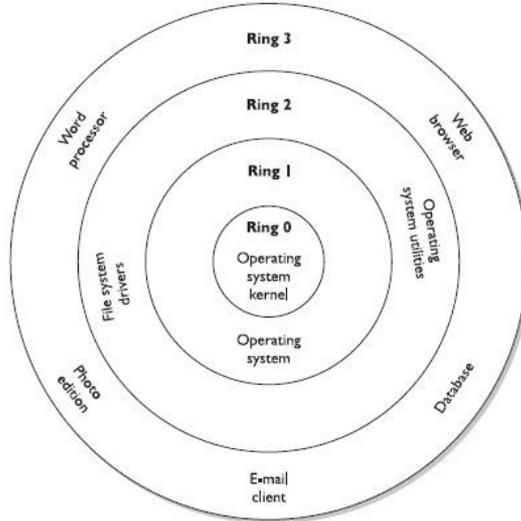




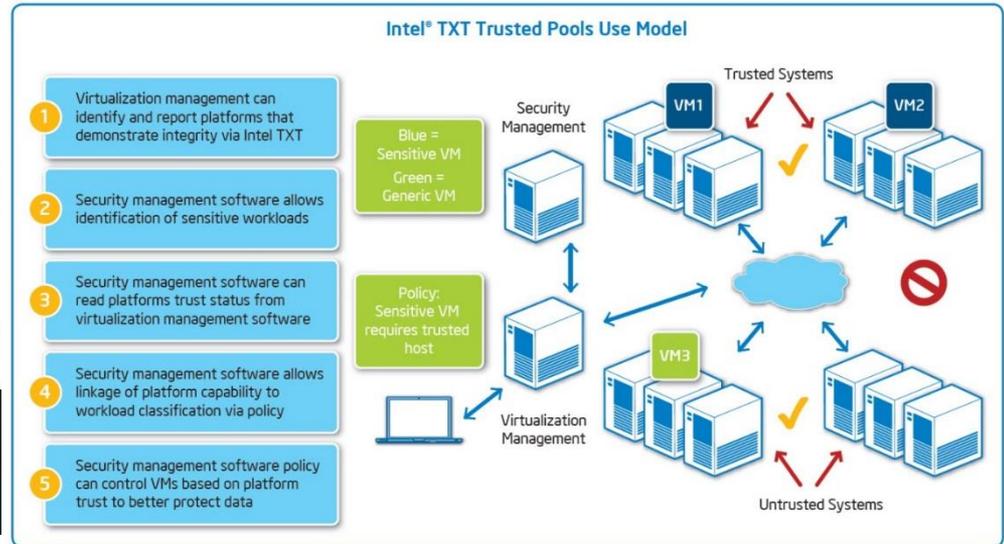
RESILIENCE TECHNOLOGIES

Intel's approach for resiliency Technology for Trust

Trusted Execution Technology (TXT)



Trusted & Verifiable Systems



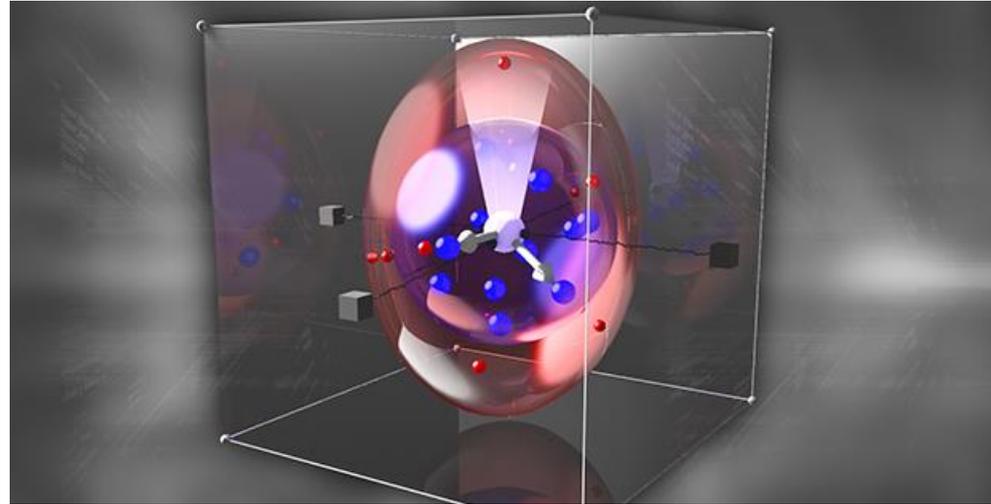


DARPA RESILIENCE TECHNOLOGIES

DARPA Seeks to Create Software Systems That Could Last 100 Years

Program aims to generate applications capable of adapting to change, without extensive reprogramming

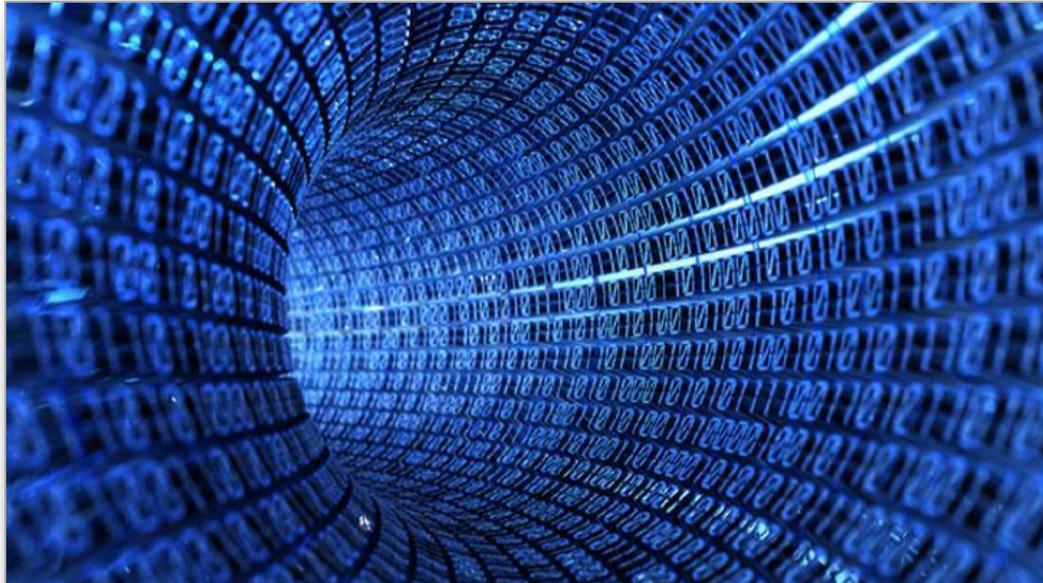
The Building Resource Adaptive Software Systems, or BRASS, program seeks to realize foundational advances in the design and implementation of long-lived software systems that can dynamically adapt to changes in the resources they depend upon and environments in which they operate.





RESILIENCE

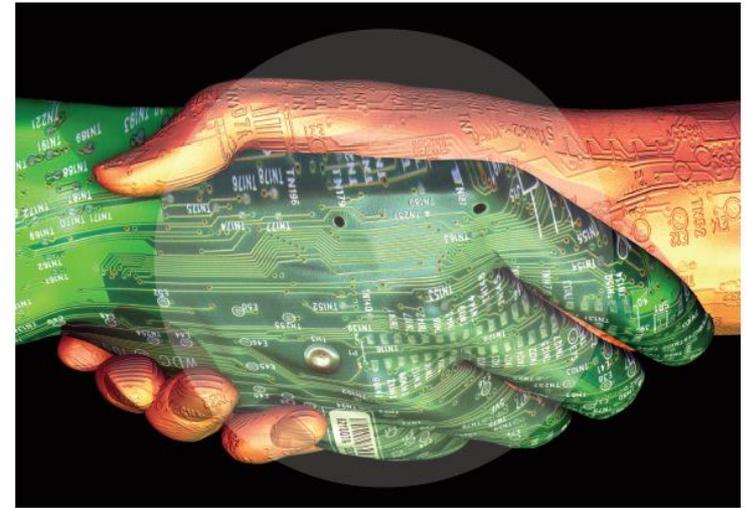
Acquisition Issues



COMMITTED TO
IMPROVING THE STATE
OF THE WORLD

Partnering for Cyber Resilience

Risk and Responsibility in a Hyperconnected World - Principles and Guidelines





RESILIENCE IN ACQUISITION

- **Resilient architecture and standards**
 - **Does the threat require a holistic approach?**
 - **Differences in securing Control Systems vs IT systems?**
 - **State of readiness for the technology?**



- **Resilience - a Systems of System and Environment Perspective**
 - **Is there a known trusted state?**
 - **Out of Band Management to return the system/enclave to a known trusted state?**
 - **Are there alternate operating modes or operating configurations?**



- **Resilience may require implementation of a technology**
 - **Can a hardware solution be implemented to your systems or enclave?**
 - **Could a reference monitor be implemented?**
 - **Could the assurance level of our hardware/software be increased?**



TAKEAWAY

- Understanding Threat & System Environment to develop your cybersecurity “Operational Resilience”
- Articulating “tradeoffs” to prioritize and grade deployment of cybersecurity capabilities
- Understanding how to “fit” into the operational environment for overall contribution to Mission Assurance

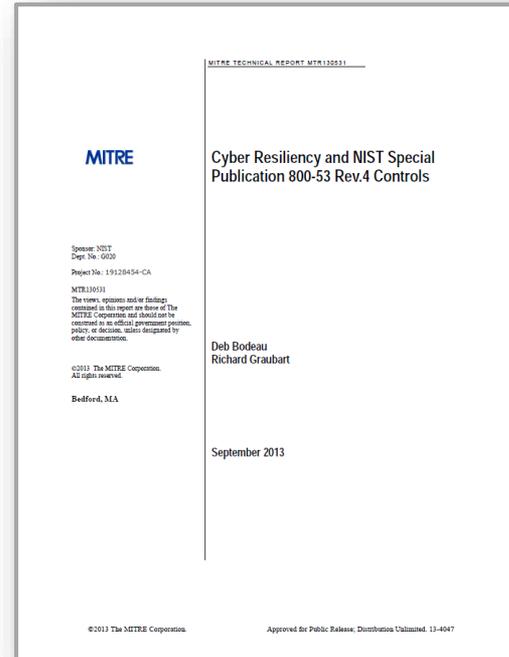
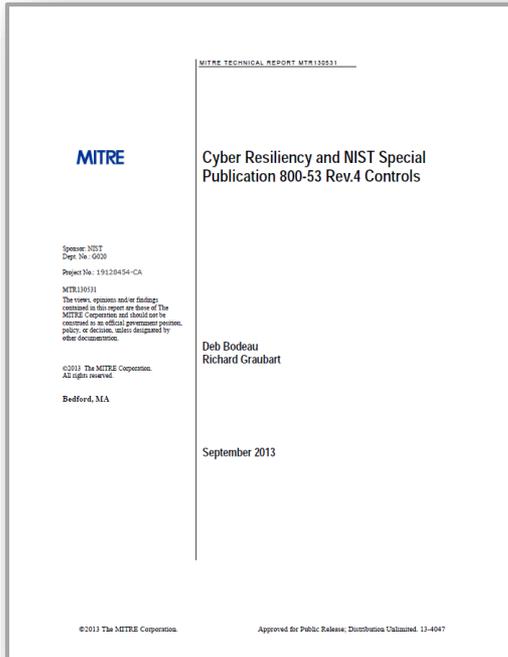




SUGGESTED READING

Cyber Resiliency and NIST Special Publication 800-53 Rev.4 Controls available at <http://www.mitre.org/sites/default/files/publications/13-4047.pdf>

Cyber Resiliency Engineering Framework available at http://www.mitre.org/sites/default/files/pdf/11_4436.pdf





SUGGESTED READING

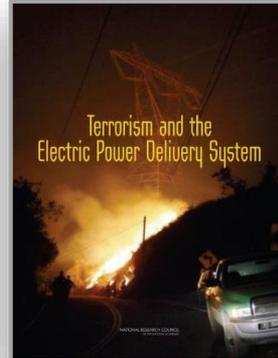
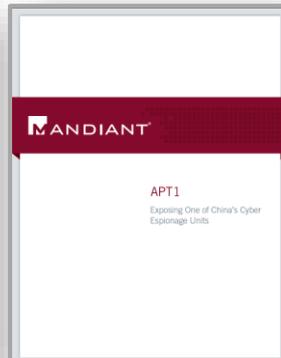
The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure available at https://project2049.net/documents/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf

APT1 Exposing One of China's Cyber Espionage Units available at http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

Terrorism and the Electric Power Delivery System available at http://www.wiresgroup.com/docs/reports/WPF_Terrorism%20and%20The%20Electric%20Power%20Delivery%20System.pdf

20YY Preparing for War in the Robotic Age available at http://www.cnas.org/sites/default/files/publications-pdf/CNAS_20YY_WorkBrimley.pdf

Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies available at http://www.cnas.org/sites/default/files/publications-pdf/CNAS_PoisonedFruit_Danzig_0.pdf





SUGGESTED READING

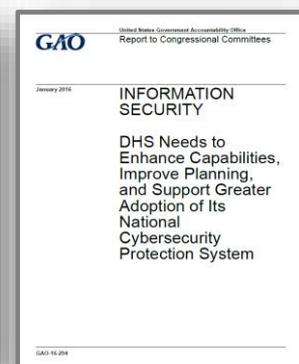
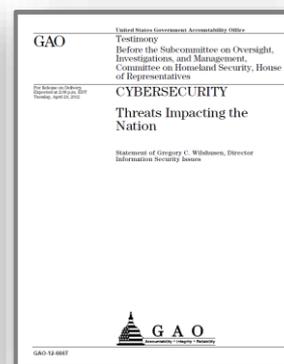
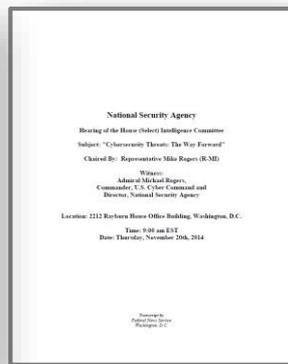
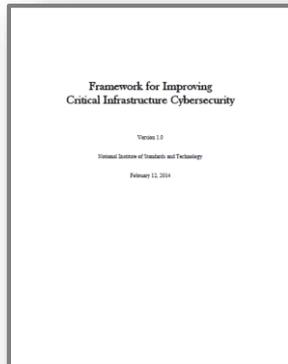
Framework for Improving Critical Infrastructure Cybersecurity Version 1.0 National Institute of Standards and Technology available at <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf>

Cybersecurity Threats: the Way Forward available at https://www.nsa.gov/public_info/files/speeches_testimonies/ADM.ROGERS.Hill.20.Nov.pdf

Cybersecurity of the Nation's Electric Grid Requires Continued Attention available at <http://www.gao.gov/assets/680/673245.pdf>

Cybersecurity Threats Impacting the Nation available at <http://www.gao.gov/assets/600/590367.pdf>

DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System available at <http://www.gao.gov/assets/680/674829.pdf>





SUGGESTED READING

The DoD Cyber Strategy available at http://www.defense.gov/home/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

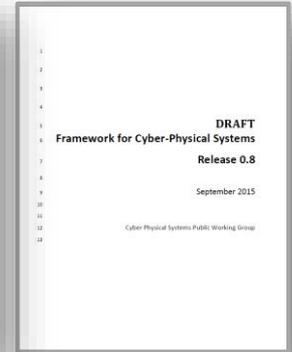
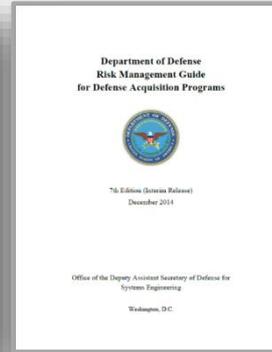
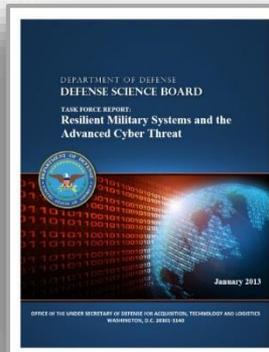
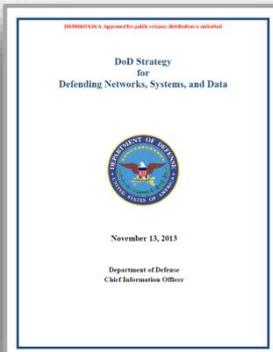
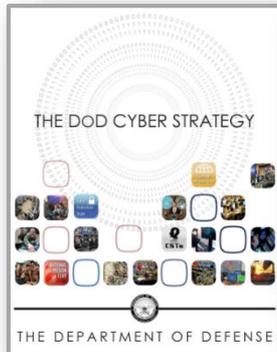
DoD Strategy for Defending Networks, Systems, and Data available at <http://dodcio.defense.gov/Portals/0/Documents/DoD%20Strategy%20for%20Defending%20Network%20Systems%20and%20Data.pdf>

Resilient Military Systems and the Advanced Cyber Threat available at <http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf>

Technology and Innovation Enablers for Superiority in 2030 (Defense Science Board) available at <http://www.acq.osd.mil/dsb/reports/DSB2030.pdf>

Department of Defense Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs available at <http://bbp.dau.mil/docs/RIO-Guide-Jun2015.pdf>

(Draft) Framework for Cyber Physical Systems Release 0.8 available at <http://www.cpspwg.org/Portals/3/docs/CPS%20PWG%20Draft%20Framework%20for%20Cyber-Physical%20Systems%20Release%200.8%20September%202015.pdf>





SUGGESTED READING

Industrial Internet Reference Architecture (Industrial Internet Consortium) available at
<http://www.iiconsortium.org/IIRA.htm>

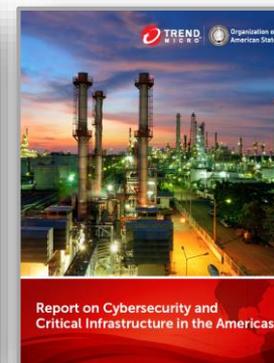
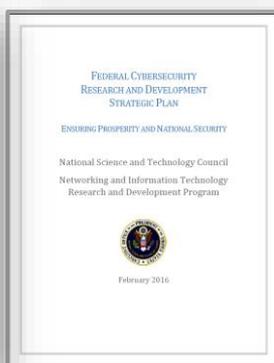
Federal Cybersecurity Research and Development Strategic Plan available at
https://www.whitehouse.gov/sites/whitehouse.gov/files/documents/2016_Federal_Cybersecurity_Research_and_Development_Strategic_Plan.pdf

Risk Nexus Overcome by cyber risks? Economic benefits and costs of alternate cyber futures available at
<http://publications.atlanticcouncil.org/cyber risks/risk-nexus-september-2015-overcome-by-cyber-risks.pdf>

Cyber Benefits and Risks: Quantitatively Understanding and Forecasting the Balance at
<http://pardee.du.edu/sites/default/files/Cyber%20Risk%20Pardee%20Extended%20Report.pdf>

Report on Cybersecurity and Critical Infrastructure in the Americas available at
<http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/critical-infrastructures-west-hemisphere.pdf>

Partnering for Cyber Resilience available at http://www3.weforum.org/docs/WEF_IT_PartneringCyberResilience_Guidelines_2012.pdf





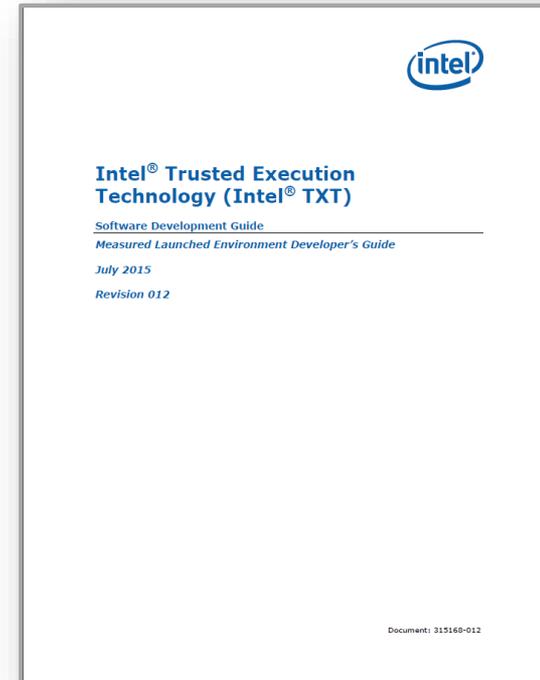
SUGGESTED READING

Task Force Cyber Awakening (TFCA) Overview available at

http://www.afcea.org/events/navyday/15/documents/IDIndustryDayTFCAOverview_releasable.pdf

Intel® Trusted Execution Technology (Intel® TXT) available at

<http://www.intel.com/content/dam/www/public/us/en/documents/guides/intel-txt-software-development-guide.pdf>





Questions